PUBLIC SAFETY SPECTRUM: HOW MUCH DO WE NEED FOR DATA?

Prepared By
The Spectrum Coalition for Public Safety
www.spectrumcoalition.org

October 25, 2005

SPECTRUM COALITION
FOR PUBLIC SAFETY

1. Executive Summary

Local, State and Federal governments, and more specifically our public safety organizations, are the groups the public relies on to protect their lives and property in time of disaster. These same organizations work to thwart disaster and to provide early warning. Broadband wireless connections to public safety personnel, wherever their work takes them, are an increasingly important tool for public safety. The need and benefit will only grow by orders of magnitude with time. Ten years ago, we wouldn't have been able to fathom what private citizens, governments and corporations, now do over the Internet…using both wired and wireless access technologies. It is now time to bring such connectivity to critical public safety and first responder organizations. With a mobile broadband wireless foundation, public safety operational innovations are also expected to take advantage of this capability in the same manner. Radio frequency spectrum is the foundation for mobile broadband wireless.

The following report represents the Spectrum Coalition for Public Safety's contribution to the decision regarding how much spectrum is required to support the public safety wireless data needs. Letters of support from organizations supporting the positions and findings in this report are attached or are available online at www.spectrumcoalition.org. This paper is based on the real-world experience of the District of Columbia, a Spectrum Coalition member, operation of a city-wide broadband network and utilizing broadband data applications over that network, such as streaming real-time video since January 2005.

Specifically, this paper looks at the upper 700 MHz band spectrum currently allocated to the Commercial Mobile Radio Service (CMRS) and designated, at some future time, for competitive bidding[1]. Currently this spectrum remains allocated to commercial television broadcasting. Within the CMRS allocations, two blocks (Blocks C and D) remain unassigned by competitive bidding. Taken together, these two blocks equal 30 MHz of available spectrum. The goal is re-allocation of CMRS fixed/mobile to Public Safety (PS) and to obtain Federal, State and local broadband interoperability access to upper 700 MHz as new Federal, State, and local *shared* frequency allocation with Primary PS fixed/mobile/aeronautical mobile status nationwide for joint shared use.

Many new public safety applications, particularly video applications, have been developed in the months following the attacks that destroyed the World Trade Center and seriously damaged the Pentagon. These threats to our nation are so serious that a cabinet level department has been created in the Federal Government to better deal with Homeland Security matters. We learned significant lessons from the event of September 11, 2001. It would be a grave error to make the same mistakes twice. Today, public safety must rely on images of an incident from broadcast news. These news agencies can not enter dangerous areas that would risk further injury. Further, public safety is reliant on what these broadcast organizations deem as important to their viewers, not what is important to saving lives and property. These are lessons learned at the World Trade

[1] Details contained in the Balanced Budget Act of 1997

Center[2], the Pentagon, and most recently from Hurricane Katrina. Additionally, our Federal homeland security officials require the same tools, and importantly, in-band frequency *interoperability*[3] with State and Local organizations and officials. Therefore, it is critical that this spectrum allocation account for Federal use, and as a result, this paper addresses Federal, State and local broadband wireless demand. The introduction of Federally mandated incident management tools such as the Incident Command System (ICS) and the National Incident Management System (NIMS) will add to the network demands[4]. The NIMS architecture also requires on-site communications servers making it difficult or impossible to leverage commercial wireless services[5].

Management of radio spectrum has not kept pace with these events and today continues to move down a path in which the most suitable spectrum is likely to be auctioned. Congress must carefully weigh its options – it can take a small piece of the national debt off the table in the short term, or leave public safety crippled for decades if not forever. The availability of upper 700 MHz spectrum presents a unique opportunity for Congress and public safety to address these needs. If Congress does not grant wide-area, broadband capabilities today, we see no additional spectrum or advanced technology on the horizon that can satisfy the broadband wireless gap. The time to act is **now**.

This paper outlines the expected demand for broadband wireless capabilities[6]. It addresses applications that public safety has identified as critical for the immediate future. These applications provide wireless interoperable communications that allow public safety users to easily and quickly share information with other agencies *at all levels* of government during times of crisis (whether man-made or natural), wirelessly share nationwide alerts, images, data files or streaming video of immediate security threats, transmit and receive video, images and/or data to critical off-site subject experts, transfer biometric information and allow two way internet and intranet access to ensure real-time decision making.

This paper accounts for the best-in-class bandwidth management (or compression) techniques as well as the networking technologies that provide the most efficient use of spectrum. While new algorithms and techniques will be identified daily, these improvements will be absorbed by increases in the quantity of communication and

[2] See the 9/11 commission report for specific details of the lack of communications capabilities at the World Trade Center complex.

[3] *Interoperability*: An essential communications link within Public Safety and public service wireless communications systems which permits units from two or more different agencies to interact with one another and to exchange information according to a prescribed method in order to achieve predictable results.

[4] More information available at: http://www.fema.gov/news/newsrelease.fema?id=15556 for ICS and http://www.fema.gov/nims for NIMS.

[5] For additional information regarding the use of commercial wireless services for public safety, see the Spectrum Coalition filing to the Federal Communications Commission request for comment, No. 05-80 / WT Docket No. 05-157. http://www.spectrumcoalition.dc.gov/img/Spectrum%20Coalition%20Comments%20FCC%2005-80%20final.pdf.

[6] To include mobile and aeronautical mobile.

the quality. Therefore, just as today's computing world soaks up the additional computing power of today's processors with improved capabilities, tomorrow's broadband wireless capabilities will follow the same trend.

Three demands must be met by the ultimate broadband network: the demand of an individual user (how much throughput is needed by one individual), the demand of an individual network site (how much concentrated use exists at a single or clustered incident), and the demand of an entire municipal public safety network, all for downlink and uplink paths[7]. All three of these demands are investigated in this report, but the individual transceiver site demand represents the deciding criteria for the amount of spectrum needed for public safety broadband requirements. The expected demand on an individual site is roughly 12.5 Mbps[8].

Spectrally efficient technologies must be able to accommodate that demand within the broadband spectrum allocation designated from Congress and implemented by the FCC. Therefore, this paper investigates the leading technologies that provide spectrally efficient broadband wireless communications. In choosing the consideration set for these technologies, only affordable COTS technologies have been selected. While other technologies may be more spectrally efficient, they are not widely available or expected to have significant economies of scale. The resultant spectral efficiency of the best technology is 1.2 bits per seconds per Hertz[9] at an individual transceiver site.

The net result is 25 MHz[10] of spectrum required to meet the base capacity requirements. However, this is not the entire picture. The coverage at 700 MHz will be vastly superior to much higher frequencies and will enable public safety to afford its operations. However, even 800 MHz voice systems require additional tools to enhance coverage and mitigate risks. For this reason, 5 MHz of additional spectrum is needed to accommodate vehicular repeaters and peer-to-peer communications.

It is then recommended that **30 MHz of additional spectrum, comprising the C and D blocks in the upper 700MHz band, be permanently reserved and allocated for shared use of local, regional and federal public safety use.** Public safety has already requested additional spectrum to accommodate this need in the PSWAC report. Congress, not the FCC, is the gatekeeper on competitive bidding, and *must* deliver on this request and address the long anticipated need for public safety spectrum.

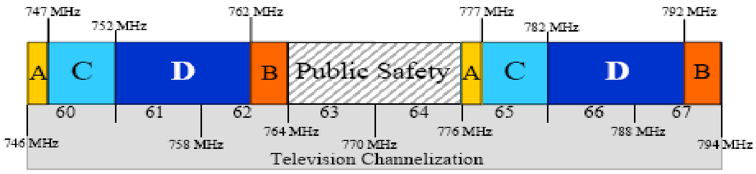
[7] The downlink (otherwise known as forward or download) path is from the base station to the wireless subscriber device (e.g. computer modem). The uplink path is from the subscriber device to the base station or other system wireless access point and is also known as the reverse path.

[8] This represents the more limiting forward or downlink path demand on the site.

[9] This is the downlink spectral efficiency – the throughput of the downlink path for a Frequency Division Duplex technology.

[10] Includes incremental capacity (can not deploy ½ or some fraction of a channel), a corresponding uplink allocation, and guard bands to avoid interference.

Upper 700 MHz Bandplan



Block	Frequencies (MHz)	Bandwidth	Pairing	Geographic Area Type	No. of Licenses
A (Guard Band)	746-747, 776-777	2 MHz	2 x 1 MHz	Major Economic Areas	52
B (Guard Band)	762-764, 792-794	4 MHz	2 x 2 MHz	Major Economic Areas	52
C	747-752, 777-782	10 MHz	2 x 5 MHz	700 MHz EAG	6
D	752-762, 782-792	20 MHz	2 x 10 MHz	700 MHz EAG	6

2. Objective

On September 11th, 1996 the Public Safety Wireless Advisory Committee (PSWAC) made a number of observations and recommendations in their Final Report[11] to the Federal Communications Commission and the National Telecommunications and Information Administration. One of the key recommendations has been partially implemented, allocation of 24 MHz in the 700 MHz band. This is a good start, but unfortunately almost a decade later the spectrum is still encumbered by television broadcasters in most markets, precluding wide-scale roll-out of additional voice and wideband data services for first responders.

The Final Report further recommended that "over the next 15 years, as much as an additional 70 MHz of spectrum will be required to satisfy the mobile communications of the Public Safety community", but this **has not occurred**. The additional spectrum that has been allocated in the 4.9 GHz band is limited in functional use and provides only local area or hotspot broadband capabilities.   Especially in areas like the National Capitol Region it is critical that local, state, and Federal officials and first responders have interoperable communications. There exists no better way to accomplish this but to be co-located in frequency and spectrum utilization. This report addresses that need and co-locates it with an overall broadband spectrum assignment for shared Federal, state, and local government public safety.

There is a real risk that the best spectrum for these purposes will be auctioned unless Congress acts now to direct the FCC to reserve this resource for the public good.

[11] Final Report of the Public Safety Wireless Advisory Committee to the Federal Communications Commission, Reed E. Hundt Chairman, and the National Telecommunications and Information Administration, Larry Irving, Asst. Secretary of Commerce for Communications and Information, September 11, 1996

Once gone, it is unlikely that any spectrum with these coverage and propagation qualities will ever be available for Public Safety.

This document outlines the requirements for public safety justifying this recommendation in terms of coverage, throughput, and cost effectiveness. Much of this information is based on the experiences derived in use of the experimental broadband wireless public safety data network[12] deployed in the District of Columbia.

3. Baseline requirements

The following sections outline the baseline requirements for coverage and capacity for public safety broadband wireless communications. These two factors set the stage to determine the band necessary for wireless transmission and quantify the amount of bandwidth required in that band.

3.1 Coverage requirements

Coverage requirements for public safety networks are not the same as for commercial wireless networks. Because these public safety networks must be as available as possible, the design and engineering of these networks is more complex and the resulting networks must be more robust. Where commercial operators will be satisfied with some level of in-building coverage, public safety needs 100% communications. Additionally, public safety usage is very concentrated and needs to be accommodated in the depths of buildings and in remote places of the country. We can not predict where broadband communication is needed, and therefore, we must provide an infrastructure that provides the greatest reach for typical use, and backup systems for all situations. Furthermore, high mobility including the ability to communicate at high speeds as well as transparent site-to-site transition is mandatory.

3.1.1 Wide area

Networks built to provide communications services for police, fire and Emergency Medical Services (EMS) must work equally well in **all areas** served by the first responder. It is impossible to predict where the next emergency will take place or, for that matter, the nature of the emergency driving network "demand". In essence, public safety needs the same wide area coverage achieved from voice networks in its broadband data networks. As the preponderance of radios (not networks), and therefore users, are in the 800 MHz band, similar coverage is required with these broadband networks.

Some voice networks are designed for outdoor coverage and seek peer-to-peer or vehicular repeater solutions to provide in-building service. Other public safety networks provide the majority of coverage, including in-building, via tower/rooftop sites. These decisions are largely made due to financial limitations. The same principals will likely apply to broadband networks. However, the same fundamental fact will prevail – that

[12] Wireless Accelerated Responder Network (WARN)

public safety will need to leverage the existing radio network infrastructure (i.e. the sites) in order to minimize operational costs. Therefore, we must make every attempt to achieve the needed network coverage from the existing constellation of 800 MHz sites.

Additionally, we must address the communication need to span wide areas. While it is vitally important to be able to communicate among personnel at an incident, it is equally important that the situation be communicated back to remote or command officials providing additional support. Therefore, the network must consist of interconnected and ubiquitous nodes with the Internet (or a private, government, part of the Internet) as its hub. This infrastructure will provide the needed interoperability across the country.

Initially, it may not be achievable to provide the same level of coverage with the same number of sites (voice communications is far less bandwidth intensive than broadband data, and for a variety of factors, coverage is not as good with broadband wide-area systems as it is with narrowband voice systems). For this reason, it is important to have deployable base stations to augment coverage, partner with commercial operators, and to leverage improvements in the core technologies (such as smart antennas) to eventually make up the difference.

3.1.2 Incident communications

A significant amount of public safety communications is incident related. The incident can span a metropolitan area (e.g. the sniper that plagued the Washington, DC area) or a single building (e.g. a large building fire or hostage situation).

While a significant portion of today’s voice traffic is for local/incident consumption, most of today’s data traffic is for remote consumption. Most applications that exist today require connectivity back to centralized servers and the data that is shared is used predominately by remote personnel. Therefore, the coverage for any broadband network must extend the vast capacity of an incident to the remainder of the network – whether the recipients of such information are servers, desktop users, or broadband wireless users in the field.

Additionally, incident work, such as firefighting, takes first responders into the depths of large buildings. Therefore, in-building broadband coverage is a critical need for public safety and is addressed in the following section.

It is important to note that in the foreseeable future, inexpensive, wearable, and rugged cameras could be deployed to share video information between firefighters and emergency response team members. This will require that public safety personnel be able to communicate across the incident area – including in-building to outdoor coverage.

3.1.3 Indoor

Indoor, also referred to as in-building coverage, is important for operational public safety communications systems. There are several potential approaches to indoor coverage, none of which is particularly satisfactory (as they stand today).

Additional 700 MHz sites could be deployed in the service area which will have the effect of increasing signal strength in the vicinity of the incident. However, this will have limited impact in providing comprehensive core building coverage over wide areas and will put a significant capital and operations burden on governments across the country.

In-building systems, including "leaky cable" or micro cells, could dramatically improve signal coverage, but must be in place prior to an emergency. These type solutions lend themselves best to public buildings with large numbers of occupants (i.e. schools, hospitals etc.) which would make this sort of system enhancement more cost effective. However, these systems are extremely expensive to build and maintain, and, with only sporadic use, are much more difficult to remain operational. The best systems are used daily and continually and are always ready for an emergency.

Another potential solution is the mesh network "bread crumb" approach. With this system, which can work in licensed (4.9 GHz) and unlicensed (2.4 GHz and 5.3 GHz) bands, first responders drop miniature radio repeaters as they work their way into a building and each "chains" with the others along the trail to carry the signal to the user. We need our first responders to focus on their core responsibilities, not creating ad hoc networks at the incident. While *ad hoc* or mesh networks are an important solution to provide more reliable communications, they should not be relied upon for the primary communication mechanism in this case. Additionally, it is unwise to rely on unlicensed frequencies where consumers could legally interfere with public safety communications.

The requirement for in-building data coverage is then the same level of coverage that public safety demands of its voice networks. This level of coverage is not currently achievable with broadband wireless wide-area technologies today, or in the foreseeable future. As a result, an alternative, such as vehicular repeaters at 700 MHz is needed.

3.1.4 Peer-to-peer

No single wireless network will provide 100% coverage. Vehicular repeaters may not be immediately on scene and even vehicular repeaters won't solve all coverage needs. Therefore, on incident peer-to-peer communications is necessary. While the data applications to support peer-to-peer communications are rare, we must provide a foundation for this communication to occur. It is also important to not rely solely on peer-to-peer communication. While it is a viable backup, if not interconnected with the core network, only local users can receive information, these users are often occupied with their own efforts and remote monitoring of the event often plays the role of identifying downed firefighters and other such events. Therefore, peer-to-peer networking plays an important, but not unitary, role in the communications architecture.

3.2 Throughput requirements

The following sections outline the amount of total demand required for public safety. The individual needs of a single public safety representative, the collective needs of users accessing the same base station, and the aggregate use across the entire municipality are the core drivers the quantity of public safety spectrum needed. The key driver for the amount of spectrum is the amount of throughput, measured in kilobits per second (kbps) or megabits per second (Mbps) required for each case. If the network can not support the throughput required by public safety use, such insufficient capacity can have significant impacts on the delivery of beneficial information, from unusable picture quality on a video, to excessively long download times for images.

The following sections outline the public safety throughput requirements in the three core components:

- Individual User Requirements: how much total demand, or throughput, is required of one user, or device? A user may utilize one or several applications to make up their net aggregate individual use.
- Site User Requirements: how much total demand, or throughput, is required of one wireless transmission site? A wireless transmission site will provide service to multiple users, representing multiple agencies, from multiple governments, in the same vicinity.
- Aggregate User Requirements: how much total throughput is required of users in one single jurisdiction? This usage will be made up of users from that jurisdiction and other agencies providing mutual aid.

In all cases we focus on traffic that is wide-area in nature – meaning information flow that traverses a significant portion of a jurisdiction – not just a small, incident area where 4.9 GHz spectrum may satisfy such a requirement.

3.2.1 Single user throughput requirements

Single user throughput requirements are determined by the most demanding applications. Contemplated and currently used public safety applications and the associated per data rates required to operate those applications (exclusive of IP and channel overhead) are summarized in Table 1 – *Required User Rates by Application.*

Application	***Description***	***Throughput***
Chemical/Biological /Radiological/Nuclear (CBRN) Detection System	CBRN alarms, video, and incident information from subway system	1.5 Mbps (Downlink) 10 kbps (Uplink)
Full Motion Video Including Transportation	Remote video incident monitoring at command site	300 kbps (Downlink) 300 kbps (Uplink)[13]

[13] These figures are based on usage of wireless streaming video applications in the Washington, DC pilot network. They assume the most advanced, standard video codecs (MPEG4 and H.264), VHS video

Video	& distribution of video information to patrol officers, including transportation cameras	
CAD Viewer	CAD display of emergency response vehicle status and location	50 kbps (Downlink) 3 kbps (Uplink)
EMS Ambulance Video	Transmission of patient video information for remote medical support	10 kbps (Downlink) 300 kbps (Uplink)
Scene Photos	Uploading of crime scene or traffic accident scene images.	3 kbps (Downlink) 500 kbps (Uplink)
Email / Messaging	Traditional email with limited file attachments (in both directions)	75 kbps (Downlink) 50 kbps (Uplink)
Web/Text Based Applications	Intra and inter-regional systems & cross jurisdictional database access	50 kbps (Downlink) 3 kbps (Uplink)

Table 1. *Required User Rates by Application*[14]

As depicted in the table above, the most strenuous load on the network comes from CBRN information system requiring as much as 1.5 megabits per second on the forward link. The most strenuous load on the reverse link comes from photos transmitted from the field and back to the core network. Required throughput for this application is 500 kbps for a high resolution image requiring less than eight seconds transmission time. These figures represent the user data rate, and do not include IP and other channel overhead. A twenty percent additional overhead is a common assumption in Internet engineering resulting in total throughput of 1,800 and 600 kbps for the maximum downlink and uplink throughput required per user.

While it is possible that multiple applications might be used simultaneously by a single user, it is unlikely that other applications would be used for these two worst-case applications. Therefore, we assume that the spectrum and technology must achieve the speeds of 1.8 Mbps and 0.6 Mbps for the forward and reverse links for an individual user and including overhead.

3.2.2 Sector throughput requirements (incident-centric)

resolution, and 15 frames per second (not complete full-motion, defined at 25 frames per second, but providing sufficient speed for most applications).

[14] These throughput requirements are based on measurements performed on the Washington, DC pilot broadband network.

For purposes of determining the service area of an individual sector, we assume that a 700 MHz broadband site covers the same area as existing Land Mobile Radio network sites. The number of sites to cover an area will generally depend on the building density of that area – more buildings will require more sites to provide in-building service. Public safety systems can range in size from five square miles coverage for a dense city site to hundreds of square miles for a rural site.

At any point in time, a single wireless site will have to support multiple public safety events, such as a chain of major building fires, large demonstrations, and dealing with injured coming from those demonstrations. It is the aggregation of these events and the simultaneous load placed on an individual site that creates the net throughput required of a single site.

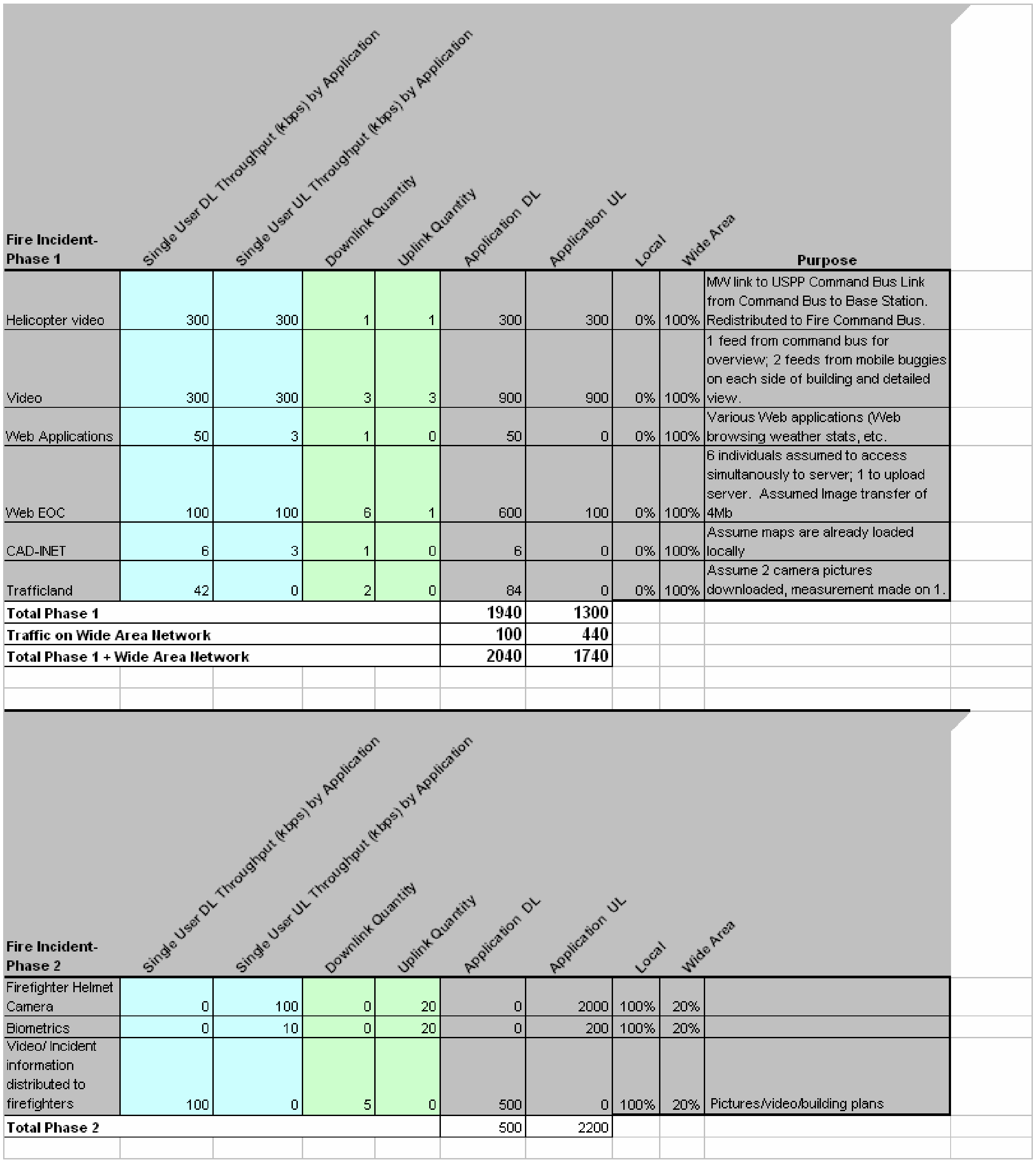
The following sections provide two single incident scenarios. In each case, the incidents can occur anywhere in the jurisdiction or network and will likely occur on a single sector, or transceiver, system. These two scenarios provide a framework for the needs of a single group of individuals associated with that incident.

Fire Incident

This incident illustrates use of public safety applications over a broadband network to support suppression of a major fire in a large building in an urban setting.

Applications used in this hypothetical incident include aerial video taken by a police helicopter and distributed to the incident Fire commander for evaluation of the conflagration and to assess resources needed to resolve the incident. Portable video cameras mounted on fire apparatus or deployed at the incident on each side of the building would provide a live detailed view of the fire, while another camera on the command bus provides an overview of the incident. Access to the internet, weather statistics, EOC and CAD applications, and traffic cameras all help first responders in addressing the incident. While not all of these applications require the bandwidth needed for video, all can be supported by a broadband wireless network (contribute to user throughput calculations) and be used by first responders on the same end user device.

System-wide throughput requirements for this scenario are a product of all individual user rates by application, multiplied by the volume of users for each application on the system. Metrics of the quantities of users and the net throughput required, for each application used in this scenario, (exclusive of IP and Channel overhead) is summarized in Table 2. – *Fire Incident*. The second section of Table 2 provides additional demand offered in the future from firefighter helmet cameras. While much of this video traffic will be needed only on a localized basis (meaning that it will be primarily shared among the firefighters at the incident), the video application may require the traffic be sent to a centralized server, or higher level command may be required to visualize some of the traffic content in a remote location thereby necessitating a significant amount of traffic be shared over a wide area. The amount of "local" traffic that becomes shared in the core part of the network is 20% in the model below, and is added to the overall incident traffic. For example, an incident commander may be the largest consumer of firefighter in-building video, however, Fire command personnel back at headquarters may review 20% of the total video generated by firefighters on the scene. Note that the video coder rate is 100 kbps for this "local" video versus 300 kbps for the higher resolution command video.



Fire Incident-Phase 1	Single User DL Throughput (kbps) by Application	Single User UL Throughput (kbps) by Application	Downlink Quantity	Uplink Quantity	Application DL	Application UL	Local	Wide Area	Purpose
Helicopter video	300	300	1	1	300	300	0%	100%	MW link to USPP Command Bus Link from Command Bus to Base Station. Redistributed to Fire Command Bus.
Video	300	300	3	3	900	900	0%	100%	1 feed from command bus for overview; 2 feeds from mobile buggies on each side of building and detailed view.
Web Applications	50	3	1	0	50	0	0%	100%	Various Web applications (Web browsing weather stats, etc.
Web EOC	100	100	6	1	600	100	0%	100%	6 individuals assumed to access simultanously to server; 1 to upload server. Assumed Image transfer of 4Mb
CAD-INET	6	3	1	0	6	0	0%	100%	Assume maps are already loaded locally
Trafficland	42	0	2	0	84	0	0%	100%	Assume 2 camera pictures downloaded, measurement made on 1.
Total Phase 1					**1940**	**1300**			
Traffic on Wide Area Network					**100**	**440**			
Total Phase 1 + Wide Area Network					**2040**	**1740**			

Fire Incident-Phase 2	Single User DL Throughput (kbps) by Application	Single User UL Throughput (kbps) by Application	Downlink Quantity	Uplink Quantity	Application DL	Application UL	Local	Wide Area	
Firefighter Helmet Camera	0	100	0	20	0	2000	100%	20%	
Biometrics	0	10	0	20	0	200	100%	20%	
Video/ Incident information distributed to firefighters	100	0	5	0	500	0	100%	20%	Pictures/video/building plans
Total Phase 2					500	2200			

Table 2. *Fire Incident*

The net result from this incident is 2,040 kilobits per second downlink and 1,740 kilobits per second uplink. This single incident may be located at cell edge, and therefore, the network must accommodate this amount of traffic at cell edge.

Metro Chemical Incident

This scenario represents a chemical incident in a subway system. It would make use of many of the same applications utilized for incident management in the fire scenario described above and would certainly rely on the CBRN application as the main information collection vehicle.

CBRN is a system developed to combat the threat of attack in the subway system, and allows integration of sensor data and video in the tunnels. It was previously only available to District first responders using hard-wired access at points fixed throughout the system. This application can now be used by the hazardous materials (HAZMAT) unit of the Fire Department with a wireless connection. This flexibility will allow the command point to be moved as near as possible to an incident - without having to know in advance where that incident will be.

System-wide throughput requirements for this scenario are a product of all individual user rates by application, multiplied by the volume of users for each application on the system. Metrics of the quantities of users and the net throughput required, for each application used in this scenario, (again exclusive of IP and Channel overhead) is summarized in Table 3. – *Subway Incident*. We again provide some future demand for helmet based streaming video and firefighter biometrics as with the scenario above.

Metro Chemical Incident- Phase 1	**Single User DL Throughput (kbps) by Application**	**Single User UL Throughput (kbps) by Application**	**Downlink Quantity**	**Uplink Quantity**	**Application DL**	**Application UL**	**Local**	**Wide Area**	**Purpose**
PROTECT	1500	10	1	0	1500	0	0%	100%	Maps, plume projection images, multiple video feeds sent to Fire and Police.
Video	300	300	1	1	300	300	0%	100%	1 feed from command bus for overview
Web Applications	50	3	1	0	50	0	0%	100%	Various Web applications (Web browsing weather stats, etc.
Web EOC	100	100	6	1	600	100	0%	100%	6 individuals assumed to access simultanously to server; 1 to upload server. Assumed Image transfer of 4Mb
CAD-INET	6	3	1	0	6	0	0%	100%	Assume maps are already loaded locally
Trafficland	42	0	2	0	84	0	0%	100%	Assume 2 camera pictures downloaded, measurement made on 1.
Total Phase 1					**2540**	**400**			
Traffic on Wide Area Network					100	440			
Total Phase 1 + Wide Area Network					2640	840			

Metro Chemical Incident- Phase 2	**Single User DL Throughput (kbps) by Application**	**Single User UL Throughput (kbps) by Application**	**Downlink Quantity**	**Uplink Quantity**	**Application DL**	**Application UL**	**Local**	**Wide Area**	
Firefighter Helmet Camera	0	100	0	20	0	2000	100%	20%	
Biometrics	0	10	0	20	0	200	100%	20%	
Video/ Incident information distributed to firefighters	100	0	5	0	500	0	100%	20%	Pictures/video/building plans
Total Phase 2					**500**	**2200**			

Table 3. *Subway Incident*

Again, as with the fire event detailed above, additional requirements will be placed in the future with firefighter biometric and video content – some of which is presented back up to the core network and represents additional demand over that core network. The subway incident presents a total of 2,640 and 840 kbps of demand on the downlink and uplink. Additionally, the network must support Internet Protocol (IP) overhead data (estimated at 20% of the total user data, or goodput[15]). The two previous scenarios then present nearly 3,200 and 2,100 kbps of net demand, or throughput, on the network at the cell edge, in the same sector.

[15] The raw data available to the user of defined as goodput, while the goodput plus all IP and other network overhead, adding 20% additional data is defined as throughput

However, as mentioned previously, the more strenuous demand is placed on the network when it must satisfy multiple incidents, simultaneously, and over a small area. The next section deals with a major terrorism event that drives such an event – one where multiple simultaneous incidents, and their ensuing public safety responses, occur.

3.2.3 Per Site Throughput Requirements

In this scenario, we explore the impact on throughput requirements for a system-wide event consisting of significant incident that impacts communications over all of Washington, DC, but has heavy concentrations of use around multiple chemical and biological terrorist attack sites. The network must satisfy the needed throughput for the event on both the per site and overall network levels. In other words, we need to accommodate the concentration of multiple incidents that will be covered by a single site, as well as all incidents covered by all sites.

In this scenario, we assume a major above and below ground terrorism incident with a large quantity of first and second responders dealing with a significant tragedy:

- HAZMAT teams are dealing with an underground hazardous material event.
- Search and rescue teams are utilizing video to share building status and provide initial video for above and below ground damage.
- Ambulances units are streaming video to secure remote medical support from emergency room (ER) and other medical specialists (e.g. to deal with an unknown agent).
- Police units cordon off and monitor the hot zone area
- Police units monitor, via video, the progress of evacuating the contaminated area ("hot zone") and nearby areas.
- Helicopter and other police units share video information to stay informed.
- Command monitors the progress of the entire operation and constantly assesses needed and available resources
- Via email and other web based applications, emergency personnel share high-resolution images with support personnel.
- Emergency managers monitor the event and use the wireless network to help establish aid centers and distribute the needed supplies.

In order to assess the total scale of the event, we assume that the incident takes place in Washington, DC with Federal, State, and local first and second responders involved in the reaction to the event. System-wide throughput requirements for this scenario are a product of all individual user rates by application, multiplied by the volume of users for each application on the system and the percentage of simultaneous use on the system (e.g., the number of users simultaneously streaming video or clicking on a web page). Metrics of the quantities of users and the net throughput required, for each application used in this scenario, including IP and Channel overhead, is summarized in Table 4. - *Major Terrorism Incident Scenario*.

	CBRN Information System	Streaming Video	CAD Access	Web Applications	Email / Messaging
Application Rate (Goodput) Required					
Downlink Rate (kbps)	1,500	300	50	50	75
Uplink Rate (kbps)	10	300	5	5	50
Number of Users (by agency and application)					
EMA	0	35		25	25
F/EMS	50	200	50	50	50
Police		1200	200	1200	1200
Park Police (Federal)		20		35	35
Secret Service (Federal)		20			
Protective Services (Federal)		2		20	20
DHS (Other Federal)		825			
Transit Police	200	40		200	200
Total Users	**250**	**2342**	**250**	**1530**	**1530**

Goodput Per Application	CBRN Information System	Streaming Video	CAD Access	Web Applications	Email / Messaging
Peak simultaneous usage - Percent of Users (DL)	4.0%	1.5%	5.0%	5.0%	5.0%
Peak simultaneous usage - Percent of Users (UL)	4.0%	1.0%	5.0%	5.0%	5.0%
Number simultaneous Users (DL)	10	35	13	77	77
Number simultaneous users (UL)	10	23	13	77	77
Net Goodput required					
Downlink Total (kbps)	**15,000**	**10,539**	**625**	**3,825**	**5,738**
Uplink Total (kbps)	**100**	**7,026**	**63**	**383**	**3,825**

	Net Demand		Per Site Throughput Models		
Aggregate Demand (all applications)	Goodput	Throughput	Uniform Distribution	70/20 Split	80/20 Split
Downlink Throughput (kbps)	**35,727**	**42,872**	**3,572.65**	**12,504.28**	**14,290.60**
Uplink Throughput (kbps)	**11,396**	**13,675**	**1,139.60**	**3,988.60**	**4,558.40**

Table 4. *Major Terrorism Incident Scenario*

This total demand represents all simultaneous usage across Washington, DC. While such a major incident will touch all parts of the city (and extend beyond the city), most of the activity will occur in and around to the terrorist target itself. For address this concentration of public safety use, we have assumed that 70% of the above traffic is concentrated in 20% of the city. The District of Columbia government has 12 broadband sites, and therefore, 20% of the network represents 2.4 sites (covering roughly 14 square miles). One site, in this model must then accommodate 12.5 and 4.0 Mbps in the forward and reverse paths respectively. If the concentration of traffic increases, say to 80 percent of traffic in 20 percent of the network, the per site demand will increase accordingly. Given recent experience in operating the District of Columbia broadband network, the traffic is more concentrated than this conservative estimate[16].

It is important to note that in operating the pilot broadband network in Washington, DC the system capacity was reached, using in excess of 1.5 Mbps on one sector during Inauguration day from only 20 users. One agency, with only six users, streamed over 5 gigabytes of video data on that day alone. If we extend this usage out to the more than five thousand public safety personnel who operate in the District of Columbia alone, much less the surrounding jurisdictions that would come to the aid of Washington in a crisis, one can see that these estimates for usage during a major incident are quite conservative. In fact, the model shows that the demand presented to the network comprises only a few hundred simultaneous users of the many thousands of Federal, State, and local personnel who would respond to such a Washington, DC incident.

3.2.4 Summary of throughput requirements

The preceding sections outlined the throughput requirements for individual users, individual sites, and the entire network. These rates are summarized in Table 5. - *Summary of Throughput Requirements.*

	Requirement
Per user rate (derived from peak single application rate)	DL: 1.8 Mbps UL: 0.6 Mbps
Per Sector Rate (derived from single incident scenario)	DL: 3 Mbps UL: 2.1 Mbps
Per Site Rate (derived from multiple incident scenario)	DL: 12.5 Mbps UL: 4.0 Mbps

Table 5. *Summary of Throughput Requirements*

In summary, the technology and spectrum combination utilized to address these needs must be able to accommodate all three aspects of the demand presented by public safety users. The per user rate is driven primarily by the technology selected, while the per sector and per site rates are driven by the amount of spectrum and spectral efficiencies of the technology. These data will be used in Section 4.3 to calculate the total spectrum required to satisfy the public safety demand.

3.3 Cost Requirements

[16] During major events, over 90 percent of the traffic was concentrated on individual sites.

Public safety requires that the broadband wireless infrastructure be affordable now and scale to meet future needs. A number of broadband technologies provide the kind of economy of scale to make them affordable. While they are currently deployed or planned in commercial portions of the spectrum, only minor, low-cost, modifications are required to convert them to support dedicated public safety spectrum. Therefore, the solution to the public safety broadband requirement must utilize wide scale commercial off the shelf technology or technology that will soon be so. Any other assumptions about technology may lead to excessive cost and insufficient throughput or coverage.

Additionally, public safety must be able to leverage its existing assets; specifically, existing radio sites and infrastructure. A significant investment has already been made nationwide to provide voice communication capability. This existing infrastructure provides a low cost host to the needed broadband data platform.

Finally, public safety must be able to scale the capacity and coverage of the broadband solution. If technology improvements can not keep pace with the growing needs for public safety data, public safety agencies across the country must be able to scale the network by adding to the infrastructure (e.g. more sites to provide more capacity).

3.3.1 Achieve coverage using existing infrastructure

In many cases, the existing VHF, UHF, and 800 MHz radio voice and narrowband data networks provide the desired level of coverage. Many geographically large areas are served by VHF systems (e.g. statewide systems). Radio propagation improves significantly at the lower UHF and VHF frequencies; however, these allocations are configured for narrowband use and are extremely congested with critical public safety voice systems.

At the opposite end of the public safety spectrum is the existing 4.9 GHz allocation. This spectrum has far worse propagation characteristics than the other allocations. In fact, if public safety were to attempt to provide a wide area network using 4.9 GHz, estimates of 30 sites per square mile for outdoor coverage are not uncommon. For a metropolitan area that encompasses 1,000 square miles, some 30,000 sites would be required. This is an unachievable number. First, the amount of time to deploy the network would be significant. Second, it is impossible to secure the 30,000 sites in the appropriate areas to achieve coverage. Third, the cost of operating such a network is untenable.

As a result, broadband data solutions must achieve coverage largely using the existing public safety land mobile site infrastructure. Even with the best-in-class technologies, this will be difficult to achieve.

3.3.2 Scalability

As the number of users, applications, and uses of those applications grow, so must the capacity of the broadband wireless network. Not only must it be able to accommodate this growth, it must do so easily, with minimal interference or coordination with other users in the spectrum. If not, many adjacent license holders would have to reduce their coverage in order to provide the additional capacity. In essence, plug-and-play capacity and coverage enhancements are required to address long term public safety needs. Therefore, the ability for technologies to withstand self interference from internal networks or neighboring networks is a critical component to the timing of addressing capacity needs.

4. Technical Foundation of Spectrum Requirements and Spectrum Needs

Assumptions on spectral efficiency are necessary to arrive at the total spectrum need for public safety data demand. This requires matching of overall requirements to the best-in-class technologies available today. In this section we investigate these technologies and establish gaps in the off-the-shelf technologies that must be filled to satisfy public safety requirements and the resulting additional spectrum required to satisfy those requirements. Additionally, we address the spectrum band required to meet the coverage requirements outlined above.

4.1 Coverage

The 700 MHz band represents the only viable solution for wide-area broadband, public safety data needs. The 4.9 GHz spectrum allocated to public safety can meet other data communications needs, but it is not viable over wide areas. Fifteen to thirty access points per square mile are required to provide outdoor coverage at this frequency. In a small, urbanized are such as Washington, DC this represents over 2,000 access points that are both difficult to install and difficult to maintain. This issue is exacerbated when one considers the thousands of square miles in a metropolitan area and the 3.4 million square miles across the entire country. Therefore, this wide area need can not be addressed by 4.9 GHz. Additionally, due to risk of interference and loss of service from commercial users, unlicensed spectrum can not be the primary source of communications for public safety. Therefore, it is critical that the collective broadband needs for public safety be met using 700 MHz spectrum.

In today's environment we are no longer bound by traditional city, town and state borders. Public safety is required to share voice and data communications across jurisdictions and across disciplines. The technologies of yesterday cannot keep up with the demands of today. More and more today, we find ourselves requiring additional information that can be used across an enterprise of public safety practitioners. As this expands, the need for reliable, expandable and secure communications increases. This 700 MHz request will give public safety officials the spectrum they require to conduct their mission to save lives and safeguard property. As discussed above, a tremendous amount of data must be shared over wide areas in order to provide first responders the information they need to save lives and property. Furthermore, in-building communication is vital for firefighting, law enforcement, and emergency medical services and to respond to events such as those of 9/11. Finally, the 700 MHz band is synergistic with many existing public safety infrastructure. Many public safety systems in urban areas operate at 800 MHz. The existing 800 MHz infrastructures and reduced cost amplifiers that can span both bands also contribute to lower operating and capital costs for a 700 MHz deployment. Finally, all other comparable bands are occupied that can meet the coverage and capacity needs. Therefore, 700 MHz spectrum is the only viable solution.

Unfortunately, the broadband technologies available today do not have the reach or output power available in today's voice radio networks. This gap can be made up partially by the use of three high gain antennas per site, but a gap still exists. Power boosters in mobile devices may further reduce the gap. But this solution won't satisfy handheld devices that require long battery life and more portability. Even with this solution, a gap will remain and public safety will need to close this gap. Several methods can help to bridge the gap: additional spectrum allocations to reduce the amount of frequency reuse (while the technologies accommodate interference within the network and between adjacent sites, it reduces performance and coverage), the use of localized vehicular repeaters to boost the local signal and reception, use of advanced technology such as smart antennas, and peer-to-peer networks.

In addressing this shortfall, it is important to note that the capacity needs of public safety will barely be met with the remaining 30 MHz of spectrum, and therefore, no additional spectrum exists to reduce the frequency reuse (which could require triple the spectrum to accomplish).

4.2 Technology foundation driving bits/Hz

Broadband wireless technologies have made tremendous strides over the past five years. The cellular industry, Wi-Fi, and broadband Internet access have driven demand and improvements in capacity. While other technologies with greater spectral efficiency may exist, only widely available technologies are affordable, and therefore, we will only consider the leading off-the-shelf technologies. Furthermore, only technologies that meet the basic throughput requirements are considered here. The following technologies are among those considered in this analysis and all meet the needed individual user rates required in Section 3.2.1 by 2007. The minimum spectrum required in the table below corresponds to spectrum necessary to deploy contiguous sites over an area. It takes into account the channel bandwidth and the reuse factor. Most technologies below have a factor reuse of 1, meaning that the same channel can be transmitted on every sector.

	Minimum Spectrum Required[17]	***Reuse Factor***	***Maximum Throughput Per Channel***
High Speed Downlink Packet Access (HSDPA)	10 MHz (5 MHz paired channels)	1	Release 5: 14.4 Mbps DL 384 kbps UL Release 6:

[17] This excludes a guard-band. See below.

			14.4 Mbps DL 5.76 Mbps UL
1xEVDO	2.5 MHz (1.25 MHz paired channels)	1	Rev 0 2.4 Mbps DL 153 kbps UL Rev A 3.09 Mbps DL 1.8 Mbps UL Release B: 3.09 Mbps DL 3.09 Mbps UL
Wi-Max (802.16e[18])	15 MHz (3x5MHz unpaired channels)	1[19]	18.5 Mbps (DL and UL shared)
Flash OFDM Flexband[20]	7.5 MHz (3x1.25 MHz paired channels)	1[21]	3 Mbps DL 900 kbps UL

Table 6. *Minimum Spectrum Required, by Technology*

Another component to take into account is the required guard band. The guard band is defined as the spectrum between the half power points and the adjacent spectrum assignment of other network operators. It assumes that the technology must meet FCC out-of-band requirements in the 700 MHz band. Public safety would not be able to transmit in these guard bands but they are required for interference protection, and therefore, the additional guard band spectrum must be included in the overall allocation to public safety. The required guard band depends on which technology is deployed in the adjacent band. The 1xEVDO technology represents a moderate need for guard band. Less than the significant guard band that would be needed for a Wi-Max system that uses Time Division Duplex, but more than Flash-OFDM that has lower out-of-band emissions. Below are some examples of engineering guidelines for 1xEVDO:

- Between same operator-same technology: none
- Between two 1xEVDO networks: 625 kHz (on each side of the public safety allocation for both uplink and downlink blocks) or 2.5 MHz total
- Between AMPS and a 1xEVDO network: 270 kHz
- Between the NPSPAC block and a 1xEVDO network (before re-banding): 260 kHz[22]

For purposes of worst-case assumptions, we will assume CDMA to CDMA guard band size requiring 2.5 MHz of total guard band spectrum.

[18] The considered technology is the mobility version of the Wi-Max family of technologies, 802.16e, in order to accommodate the mobile public safety professionals. While this technology is not fully standardized, the assumptions herein are based on the expectation of the technology. It will not be available before end of 2006

[19] All channels are transmitted on each sector, however, three channels are required to achieve cell-edge throughput that meets the individual user requirement.

[20] This technology is not yet standardized; however, a variation of the technology has been deployed in the Washington, DC pilot network.

[21] This technology can be configured to support the same frequency reused in each site, but requires three channels to do so.

[22] Emission limits in the 800 MHz are less stringent than in the upper 700 MHz

4.3 Cell-edge performance of leading technologies

Broadband throughput varies significantly as subscriber equipment travels further from base stations. The most advanced technologies today reuse the same frequency at each site, and as a result, the strongest interference occurs at the border of the service area of two sites. A major public safety event could occur at this location in a public safety broadband network. Therefore, we must assume that this cell edge performance establishes the baseline spectral efficiency to address the public safety need and not the maximum throughput.

The most advanced technologies available today utilize three separate transceiver systems, or sectors, per site. Each sector provides its own capacity to the users operating in that sector. The sectors provide nearly triple the capacity per site, and therefore, we assume spectral efficiency is defined by three sectored transmission sites.

Based on the experience of operating a broadband pilot network in Washington, DC, it is critical to base capacity calculations on the cell-edge and not the peak or average rates. Therefore, we assume that the demand presented in Section 3.2.4 is presented to the network at cell edge. The network must provide the resources for this demand based on in this worst case capacity condition. The state-of-the-art commercial technologies for wireless broadband technologies listed in Table 6 range from 0.5 bits per second per Hertz (bps/Hz) to 1.2 bps/Hz at the cell edge, for the downlink path, and for a three sectored site. For the purposes of calculating the total spectrum required we will use the most spectrally efficient of the leading technologies, or 1.2 bps/Hz. Or, for each 1 MHz of paired spectrum, the downlink can support 1.2 Mbps at the cell edge. For a three-sectored configuration, we assume 0.6 bps/Hz for each sector.

4.4 Base spectrum required

Earlier, we outlined three types of throughput needs that must be addressed: individual user needs, site needs, and aggregate city-wide needs. Each represents a different aspect of the overall demand. The individual user need represents what any one technology is able to deliver to that user. The site needs represent the aggregate needs of users over a relatively small area (several square miles) and addresses the needs for a single incident or a collection of incidents that occur in that area.

The key driver of demand for public safety broadband is the individual site throughput. This demand of 12.5 Mbps divided by a spectral efficiency of 1.2 bps/Hz, results in 10.42 MHz required for the downlink path. However, we can not deploy partial channels, and therefore, we round up to the nearest 1.25 MHz (the smallest channel size of the aforementioned technologies), requiring 11.25 MHz. A complementary pairing of uplink spectrum as well as a 2.5 MHz guard band is also required. The net spectrum requirement is then 25 MHz to accommodate the base demand for public safety broadband data; however, as mentioned above, there are additional coverage gaps that require additional spectrum allocations.

4.5 Gaps for current technology/ additional required spectrum

The above scenarios and calculated spectrum amount provide public safety with basic wide area communication capabilities; however, it does not address several scenarios that must be considered in order to mitigate public safety risk. Specifically, in the event that the core infrastructure is unavailable (through network failure or lack of coverage) to a first responder, peer-to-peer (mobile-to-mobile) communication is required. Additionally, vehicular repeaters have proven to be a valuable asset for providing coverage in dense urban buildings. Both of these scenarios are not accommodated by the base spectrum requirement and are addressed in this section. In both cases, we assume that no additional guard band is needed between the core network frequencies and these ancillary systems.

4.5.1 Vehicular repeaters (2.5 MHz channel)

Vehicular repeaters have proven to be an effective extension to voice land mobile radio networks utilized by first responders. This capability is even more critical given the broadband coverage issues. Localized transmissions, higher power transmitters, and better receivers provide greater in-building and on-scene coverage than does the core network or peer-to-peer communications. Further, they can provide a localized capacity improvement where it’s needed most. It is important to recognize, however, that they are not a replacement for the core network capacity. They may take precious minutes to set up and are one additional link in the overall system that may reduce reliability. The overall solution needs to accommodate most scenarios without having to deploy vehicular repeaters. Vehicular repeaters for broadband networks could be deployed as transparent extensions to the core network – providing access to and from the local incident and back throughout a regional (or national) Internet Protocol network.

To achieve maximum coverage and capacity on the localized incident a dedicated broadband channel is required. This dedicated channel will operate without any interference with the core network and will provide the optimal network capability. Furthermore, interconnection from the vehicular repeater will be required to transport information to remote command officials and others. Using the same piece of spectrum would significantly degrade the on-scene throughput. The broadband 4.9 GHz spectrum may provide the coverage to reach a vehicular repeater in certain circumstances.

As detailed above, the minimum bandwidth required by any of the leading broadband technologies is 2.5 MHz; however, others require 10 MHz of spectrum at a minimum. In the interest of efficient use of spectrum, a 2.5 MHz channel size has been selected. Should public safety opt for a wider band channel (two times 5 MHz as with Universal Mobile Telecommunications System and High Speed Downlink Packet Access) subscriber devices might require dual modes (both 5 MHz and 1.25 MHz channels) to accommodate this requirement.

4.5.2 Peer-to-peer (2.5 MHz channel)

When all else fails, public safety voice radios can be switched to peer-to-peer communications. The same capability is needed for broadband data as identified in the requirements above. High-resolution streaming video will become a critical component of public safety operations. Should one or more users become detached from the network, it is critical that they retain the ability to communicate. Peer-to-peer networking provides incident area communications for first responders on the scene. In fact, this level of networking can be leveraged to connect to the core network via one or more users who are in range of the core network (including vehicular repeaters).

It is important to recognize that the demand for on-incident communication is significant. Cameras have become an essential tool available for public safety officials. These new tools come with a requirement of additional bandwidth that is in limited supply. As this the technology matures, additional requirements for daily operational needs will grow. With each new technology, demands for spectrum increase. On top of this, mesh networking among the peer-to-peer network elements will further reduce the bandwidth available to the endpoints of the network. This type of capability is a core function of Wi-Fi type technologies and is expected to be incorporated in 4.9 GHz public safety solutions. Unfortunately, propagation at 4.9 GHz is severely limited. Therefore, a 700 MHz peer-to-peer solution is required.

As with vehicular repeaters, the minimum channel size for the ultimate peer-to-peer technology becomes a significant factor to determine the total spectrum needed to support this requirement. In the case of peer-to-peer networking, it is compounded by the fact that the core "cellularized" technologies do not support peer-to-peer networking. The technology that can support that capability, Wi-Fi, requires 22 MHz of spectrum to do so. Unfortunately, the remaining 30 MHz is split in two 15 MHz pieces, and therefore, can not accommodate Wi-Fi.

Unfortunately, there is no a simple answer to solve this need. However, it must be addressed. Therefore, in order to maintain consistency with vehicular repeaters, we assume that the standard technologies operating with 1.25 MHz channels will be able to support the peer-to-peer architecture required in a separate paired channel – totaling 2.5 MHz.

5. Conclusion

We have outlined the significant need for broadband wireless communications based on experiences of operating networks and applications. We have assumed the use of highly spectrally efficient networks and applications. We have also addressed spectrally efficient ancillary systems to address the final coverage gap. What is presented here is a conservative request for an arguably limited resource.

Our country is at the crossroads for providing public safety and first responders with vital tools that will protect our country for decades. Other than the un-auctioned upper 700 MHz spectrum, there is no other spectrum that provides the needed wide-area, broadband, wireless communication is on the horizon. No magic bullet technology is available that will provide the needed bandwidth or coverage within the existing public safety spectrum allocations. No Federal public safety data communication spectrum exists and no co-located Federal/State/local/tribal spectrum exists to easily operationally tie the networks together and build a greater, national, economy-of-scale network. The demand for public safety wireless broadband communication is great and grows greater by the day. Consistent with previous requests, Congress must allocate the remaining 30 MHz of spectrum in the upper 700 MHz band for joint public safety use by Federal, state, local, and tribal entities in order to meet this demand. It is Congress which must secure a unique shared domestic spectrum allocation for nation-wide broadband data interoperability and create an environment where all public safety users can jointly operate.

Not doing so will put our first responders and those they protect at risk.